SLDS Issue Brief

How to Engage and Train Stakeholders Regarding Privacy and Security Best Practices

To successfully protect the privacy and security of individuals' data, statewide longitudinal data system (SLDS) programs must ensure that their employees clearly understand and enforce policies and practices related to privacy and security. Providing staff members with regular and appropriate training is an essential component of SLDS privacy and security measures. Investing in proper training can help SLDS programs address security threats proactively and substantially reduce the risk of data breaches and misuse of their systems.

This brief offers an overview of key concepts and content to be covered in privacy and security training for state education agencies as well as methods of delivering that content to stakeholders. It draws on best practices identified by the Privacy Technical Assistance Center (PTAC) and includes examples of privacy and security training among state agencies involved in Utah's SLDS.

Key Concepts: Goals for Data Privacy and Security Training

Education agencies increasingly rely on data—including personally identifiable information protected by the Family Educational Rights and Privacy Act (FERPA)—and data systems for internal operations, federal and state compliance reporting, and policy uses. As a result, agency employees and data users face rapidly evolving technology solutions and policy requirements that challenge their capacity to manage data safely and securely.

Effective data privacy and security training is one of the first lines of defense for agencies to protect their data. A comprehensive training program goes beyond simply making resources available to stakeholders and actively engages and supports them to create a culture of appropriate data use. Stakeholders who know how to access, manage, and use data safely help ensure that risks are identified and addressed before they result in major security incidents.

PTAC offers the following key concepts that should underpin a data security training program:

- **Raise awareness of data security in advance of formal training**. Awareness refers to the ability to perceive or be conscious of a condition or event, such as a threat to data security. An effective training program should be preceded by efforts to raise awareness of the importance of data security and potential risks to the agency so that stakeholders recognize the value in receiving more formal training and instruction.
- **Make sure that all agency employees complete training**, including new and current employees, contract workers, temporary workers, and volunteers who have access to personal data. Training should happen when employees join the organization and on a regular basis afterward. Be sure to document the delivery of training, as an audit may require evidence that training has been provided.
- **Integrate data security training with broader employee education efforts**. Like other professional development programs, data security training should be evaluated for effectiveness and its content refreshed periodically. Consider other training topics that can increase staff members' capacity and how those can be delivered to complement regular security and privacy training.
- **Develop role-based training courses** tailored to individual users' job responsibilities and level of data access.

This product of the Institute of Education Sciences (IES) SLDS Grant Program was developed with the help of knowledgeable staff from state education agencies and partner organizations. The information presented does not necessarily represent the opinions of the IES SLDS Grant Program. We thank the following people for their valuable contributions:

Jeremias Solari
Utah Data Research Center

Albert Tay
Utah State Board of Education

Eric Gray
Ross Lemke
Privacy Technical Assistance Center

Sean Cottrell
Jeff Sellers
SLDS Grant Program, State Support Team

For more information on the IES SLDS Grant Program or for support with system development, please visit http://nces.ed.gov/programs/SLDS.

ies NATIONAL CENTER FOR EDUCATION STATISTICS
Institute of Education Sciences

- **Incorporate breach detection and escalation procedures** so that stakeholders can recognize a potential security breach and escalate information to the appropriate individuals.
- **Include data security messages in all employee communications channels**. Adding security notices to internal communications such as newsletters, emails, and login reminders helps keep privacy and security issues front of mind for stakeholders.
- **Create a culture of security in the organization**. Employees' engagement in data security should not end with a required training session. Senior leaders should model a commitment to protecting data through regular engagement with staff.

Content: What Should Privacy and Security Training Cover?

The topics covered by a data privacy and security training program will vary based on the needs of the organization and the roles of the individuals being trained. However, a comprehensive training program for all employees will cover the following essential areas:

- Risk assessment, including the identification of system threats and vulnerabilities
- Physical security, such as locked doors and windows
- Desktop security, including password protection for computers and timed screen locks
- Mobile device security, including practices such as not storing sensitive data on easily misplaced storage media or accessing data on personal devices without proper oversight and security
- Network security, including secure data exchanges
- Access controls, including how to protect files with passwords, encrypt transmissions and files, and authenticate users
- Good practices related to the use of email, software, applications, and the Internet
- Phishing, hoaxes, malware, viruses, worms, and spyware
- Remote access to data and systems
- Data backup and disaster recovery
- Data security breach notification protocols
- Directions for viewing written data security procedures and principles and for asking questions about guidance in order to ensure compliance

Learn more

Read more about key concepts and content for data privacy and security training in PTAC's *Data Security and Management Training: Best Practice Considerations* (*https://studentprivacy.ed.gov/resources/data-security-and-management-training-best-practice-considerations*).

Data privacy and security training can be designed around standards that specify the knowledge, skills, and professional behaviors that stakeholders need to use data effectively and safely. Standards will cover critical knowledge for data users, including familiarity with federal and state laws as well as organization policies. Standards also can emphasize appropriate behavior for the ethical use of data, adherence to rules and laws, protection of individuals' data, and contributing to a culture of good data use. The SLDS Data Use Standards (*https://slds.ed.gov/#program/data-use-standards*) offer a framework of standards that can guide training for education data use, including topics such as

- data privacy;
- security;
- confidentiality;
- human subjects research; and
- appropriate use.

Delivery: How Will Stakeholders Receive Privacy and Security Training?

Data privacy and security training can be delivered in several ways to reach stakeholders with different goals, learning styles, skill levels, user roles, locations, and budgets. There are three common methods of delivering training:

- **On-demand training** offers a self-paced learning environment in which participants experience a course delivered by an industry expert or in-house trainer via a video or other previously developed mechanism. Employees can complete exercises at their own pace and location as long as they have access to a computer and the Internet.
- **Virtual classroom training** is delivered at specific times via web conferencing by an instructor and provides employees with remote access to classroom systems in which they can complete virtual exercises and tutorials. Because a virtual classroom offers instruction with a live instructor, this delivery method enables participants to have their questions answered and comments addressed in real time.
- **On-site training** allows organizations to have audience-appropriate training delivered at their own facilities. Training can be customized to the unique settings or circumstances of the organization, employees' responsibilities, and actual network and operational requirements of the technology environment. Some organizations reserve on-site training for more in-depth role-based training of key staff groups.

Regardless of the delivery method, it is essential that all employees participate in training. Beyond a universal training on essential privacy and security topics, more advanced training activities can be customized for different

user roles and delivered in ways that meet the schedules and work needs of those stakeholders. Stakeholders engage most strongly with training based on real-world scenarios that they might encounter in their work. Organizations can consider offering modular training courses that let users easily find the information most relevant to them, as well as providing training content in multiple formats for future reference. All training materials need to be reviewed and updated regularly to reflecting changing privacy practices, policies, and laws.

State Example: Data Privacy and Security Training in Utah

The Utah Data Research Center (UDRC), housed in the Utah Department of Workforce Services, manages an SLDS with data from across the state's education and workforce programs. UDRC adheres to the security and privacy policies and practices of the Department of Workforce Services as well as the statewide Department of Technology Services. Each state agency that contributes data to UDRC, including the Utah State Board of Education (USBE), also has its own data policies that employees and data users must follow when using data for those agencies' purposes. Some of those agency-specific policies, including FERPA compliance, translate when the data are shared with UDRC.

Key concepts for data privacy and security
UDRC tries to institutionalize and automate as many of its security and privacy practices as possible. UDRC systems de-identify data and apply secondary disclosure avoidance measures on datasets automatically. The Department of Workforce Services rules and regulations that govern UDRC were designed to comply with state directives, audit requirements, and federal regulations including FERPA.

UDRC's overarching data governance structure establishes guidelines for who can access SLDS data and how. Direct access is controlled by the Secured Access Management Service system, and UDRC personnel must approve any new requests for access to the data warehouse. External researchers requesting UDRC data must digitally confirm their agreement to follow nondisclosure practices, to allow UDRC to peer review resulting data products, and to maintain data privacy and security as well as destroy the data once their project has ended.

Beyond UDRC, other Utah state agencies implement organization-specific security measures such as encrypted computers, fob access to computers, and codes of conduct for researchers who request state data. Agencies like USBE recognize their responsibility as custodians of large amounts of data and cultivate a culture of data security.

Content of data privacy and security training
Data privacy and security are components of general training programs that Utah state agency employees must complete annually and as part of new-employee orientations. Individual state agencies offer additional training based on their own data collections and systems as well as role-based responsibilities.

At UDRC, annual data privacy and security training covers the following topics:

- Physical, desktop, mobile device, and network security practices such as preventing unauthorized access to buildings, locking computers, not writing down passwords or Social Security numbers, and handling lost ID badges
- Good practices related to the use of email, software, applications, and the Internet
- Phishing, hoaxes, malware, viruses, worms, and spyware
- Data backup and disaster recovery

Individual employees might receive additional training as required by their role, such as when receiving remote or proxy access to UDRC data and systems. Other key privacy and security topics—including identifying system threats and vulnerabilities, managing access controls, and responding to data breaches—are documented in administrative policies and incorporated into practices such as periodic risk assessments.

Agencies like USBE, which has an in-house information technology division separate from the statewide Department of Technology Services, also offer organization-specific training. All USBE employees, even those who cannot access the agency's data systems, are trained on topics like recognizing phishing scams and responding to data breaches. Data managers and researchers receive additional privacy and security training.

Delivering data privacy and security training
The Utah Department of Human Resource Management oversees annual and new-employee orientation training programs for all state personnel. Most of the training modules are on-demand videos and web applications with interactive exercises and quizzes. The Department of Human Resource Management's learning system sets timelines for completing training and tracks which employees have completed which modules. As deadlines approach, the system emails agency leaders with lists of employees who have not yet completed their training, and managers follow up with the employees on their teams.

Individual state agencies also manage and track their own training programs for employees. Some training activities are done on site and in person, especially for role-specific

responsibilities. Agency-wide emails about current threats and email scams help maintain awareness of security and privacy issues throughout the year.

Conclusion

State agencies are responsible for large amounts of data about their citizens, including sensitive personal information about students and workers. Although training programs can and should be customized to the specific data collections, technology environments, and roles in a given agency, everyone who works with and around data should receive general training related to security and privacy issues. Comprehensive training programs that provide a broad overview of security and privacy topics—along with role-specific training tied directly to employees' job duties—are essential for protecting data systems. State agencies can minimize risks to their systems and build a culture of responsible data stewardship through training programs that effectively communicate best practices and are easily accessible to users.

Additional Resources

Privacy Technical Assistance Center (PTAC)
https://studentprivacy.ed.gov/

PTAC Data Security and Management Training: Best Practice Considerations
https://studentprivacy.ed.gov/resources/data-security-and-management-training-best-practice-considerations

PTAC Data Security Checklist
https://studentprivacy.ed.gov/resources/data-security-checklist

PTAC Teacher Training Focus Groups Report
https://studentprivacy.ed.gov/resources/ptac-teacher-training-focus-groups-report

Securing Your SLDS: SLDS Issue Brief
https://slds.ed.gov/#communities/pdc/documents/15024

SLDS Data Use Standards
https://slds.ed.gov/#program/data-use-standards

Utah Data Research Center
https://udrc.utah.gov/

Utah State Board of Education
https://www.schools.utah.gov/